UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,928	09/15/2005	Guoshun Deng	CU-4207 RJS	3659

26530 7590 04/27/2010

LADAS & PARRY LLP
224 SOUTH MICHIGAN AVENUE
SUITE 1600
CHICAGO, IL 60604

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/27/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/534,928	DENG ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 May 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

I. Claim 2 has been cancelled.

II. Claims 1 and 3-21 have been examined.

III. Responses to Applicant's remarks have been given.

Response to Arguments

1. With regards to the Applicant's arguments and amendments pertaining to the 35 U.S.C. 112, 1st rejection of claim 13, said rejection is hereby withdrawn.

2. Further, the 35 U.S.C. 112, 2nd rejection of claims 4, 6, 9, 10, 12, 13, 18, 19 and 21 is also hereby withdrawn based upon the Applicant's amendments to said claims.

3. Further, the objection to the disclosure and to claims 1, 14 and 16 is also hereby withdrawn.

4. Regarding the Applicant's arguments pertaining to the storage of an algorithm, said arguments are moot in view of Lys providing the necessary storage means within the new grounds of rejection, as cited below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1 and 3-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 6,272,631 to Thomlinson et al., hereinafter Thomlinson, and further in view of United States Patent No. 6,717,376 to Lys et al., hereinafter Lys.

5. Regarding claim 1, Thomlinson teaches wherein the semiconductor memory device comprises a controller module as well as a universal interface module and a semiconductor storage medium module electrically connected with the controller module, respectively, characterized in that the method comprises the steps of: dividing the semiconductor storage medium module into at least two logic memory spaces (column 4, lines 45-55, "system memory includes read only memory (ROM) 24 and random access memory (RAM) 25" and column 7, lines 25-32, "a dynamically linked library (DLL) that can be executed in the application programs' address spaces"); using at least one of the logic memory spaces for storing the data to be protected (column 2, lines 16-23, column 3, lines 7-15, column 6, lines 10-35, "the protected storage system allows application programs to securely store data items that must be kept private and free from tampering", column 7, lines 15-21, "the protected storage system is implemented in a different address space than the calling application programs", column 9, lines 31-43 and column 11, lines 28-35);

setting up and storing a password for the semiconductor memory device and said at least one logic memory space (column 2, lines 37-44, column 6, lines 10-25, column 8, lines 53-58, 66 and 67, column 9, lines 1-6 and 31-58 and column 10, lines 33-38); certifying the password before read/write operation; when writing the data to be protected in the semiconductor memory device, the controller module receiving the data from the universal interface and, after encrypting the data, storing the encrypted data in the semiconductor storage medium module (column 2, lines 28-44 and 60-67, column 3, lines 1-21, column 4, lines 45-67, column 5, lines 1-18, column 6, lines 10-39 and 47-53, column 7, lines 41-53, column 9, lines 31-37 and 59-63 and column 10, lines 1-14 and 30-50, "the storage server stores the encrypted individual data item, the item authentication code, the encrypted item key, the encrypted item authentication key, the key authentication code, the encrypted master key, and the encrypted master authentication key, to be retrieved later when requested by an authorized application program");

and when reading the data to be protected from the semiconductor memory device, the controller module decrypting the data and transmitting the decrypted data via the universal interface (column 3, lines 12-15, column 6, lines 47-53 and column 9, lines 31-47 and 59-65).

6. Thomlinson significantly teaches the claimed invention, as cited above. However, Thomlinson does not sufficiently teach the claim language pertaining to algorithm storage. Lys teaches said claim language, as cited below.

7. Regarding claim 1, Lys teaches a method for realizing data security storage and algorithm storage by means of a semiconductor memory device, wherein at least one of the logic memory spaces is for storing an algorithm, the controller module executes a designated algorithm according to input data from the universal interface and transmits a result of the execution via the universal interface (column 16, lines 6-16 and column 18, lines 36-49).

8. The motivation to combine would be provide a means "to select a program from memory, modify a program from memory, modify a program parameter from memory, select an external signal or provide other user interface solutions." (*Lys* – column 16, lines 13-16).

9. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Lys with the teachings of Thomlinson to provide a means to store the appropriate instructions to execute various functions.

10. Regarding claims 3 and 15, Thomlinson teaches that the semiconductor storage medium module comprises a storage medium, *or* a combination of at least two storage media (column 2, lines 16-23, column 3, lines 7-15, column 6, lines 10-35, "the protected storage system allows application programs to securely store data items that must be kept private and free from tampering", column 4, lines 45-55, "system memory includes read only memory (ROM) 24 and random access memory (RAM) 25", column 7, lines 15-32, "the protected storage system is implemented in a different address space than the calling application programs" and "a dynamically linked library (DLL) that

can be executed in the application programs' address spaces", column 9, lines 31-43 and column 11, lines 28-35).

11. Regarding claim 4, Thomlinson teaches that the semiconductor memory device and said at least one logic memory space set up at least two levels of users passwords (column 7, lines 64-67, column 8, lines 1-29 and 41-57 and column 9, lines 1-6 and 31-49).

12. Regarding claim 5, Thomlinson teaches that certification of user passwords is implemented before operation in all logic memory spaces, *or* before operation in the logic memory spaces storing the data to be protected (column 8, lines 53-67 and column 9, lines 1-11 and 31-58, "wherein data items are encrypted based on a user-supplied password, or some other code related to user authentication, before storing the data items").

13. Regarding claim 6, Thomlinson teaches setting up a database, and conducting access and authority management to the data to be protected by way of the database (column 3, lines 7-15, column 6, lines 10-29 and 40-53 and column 7, lines 15-32).

14. Regarding claim 7, Thomlinson teaches that the authority comprises reading authority, writing authority, modifying authority, deleting authority and executing authority, each authority having the meanings of:

Reading authority: only allowing reading record data in the database; Writing authority: only allowing writing new data in the database, but not covering the record data with the same record title (column 8, lines 1-9, "read and write access");

Modifying authority: only allowing writing data in the database and covering the record data with the same record title (column 8, lines 46-52, “the user can later modify access rights to the data”);

Deleting authority: allowing deleting the database or records therein (column 27, part of the IPStore Interface, "DeleteItem", "DeleteSubtype" and "DeleteType");

Executing authority: allowing executing record codes in the database, which is an authority with respect to a self-defined algorithm or function code and it is invalid to designate an executing authority for normal record data (column 8, lines 53-67 and column 9, lines 1-11 and 31-58, “wherein data items are encrypted based on a user-supplied password, or some other code related to user authentication, before storing the data items”).

15. Regarding claim 8, Thomlinson teaches that at least one of the logic memory spaces is used for storing data that does not need protection (column 4, lines 45-67 and column 5, lines 1-20).

16. Regarding claims 9 and 18, Thomlinson teaches in that an anti-falsifying identification is performed to identify whether the transmitted *or* stored data is falsified or not (column 9, lines 20-28 and column 11, lines 4-10).

17. Regarding claims 10 and 19, Thomlinson teaches that during transmitting or storing data, *the anti-falsifying identification* comprises the steps of:

A. invoking an encrypting algorithm to convert original data to obtain a conversion value X (column 2, lines 28-44 and 60-67, column 3, lines 1-21, column 4, lines 45-67, column

5, lines 1-18, column 6, lines 10-39 and 47-53, column 7, lines 41-53, column 9, lines 31-37 and 59-63 and column 10, lines 1-14 and 30-50);

B. packing the original data and the conversion value X according to a format to form a data package (column 3, lines 7-15, column 6, lines 10-29 and 40-53 and column 7, lines 15-32);

C. transmitting *or* storing the data package (column 2, lines 16-23, column 3, lines 7-15, column 6, lines 10-35, "the protected storage system allows application programs to securely store data items that must be kept private and free from tampering", column 4, lines 45-55, "system memory includes read only memory (ROM) 24 and random access memory (RAM) 25", column 7, lines 15-32, "the protected storage system is implemented in a different address space than the calling application programs" and "a dynamically linked library (DLL) that can be executed in the application programs' address spaces", column 9, lines 31-43 and column 11, lines 28-35);

and during receiving or reading data, the anti-falsifying identification comprises the steps of:

A. unpacking the data package according to the format to obtain the unpacked original data and the conversion value X (column 3, lines 12-15, column 6, lines 47-53 and column 9, lines 31-47 and 59-65);

B. invoking the encrypting algorithm to calculate a conversion value of the unpacked original data to obtain a conversion value Y (column 2, lines 28-44 and 60-67, column 3, lines 1-21, column 4, lines 45-67, column 5, lines 1-18, column 6, lines 10-39

and 47-53, column 7, lines 41-53, column 9, lines 31-37 and 59-63 and column 10, lines 1-14 and 30-50);

C. comparing the calculated conversion value Y and the conversion value X to see whether they are equal to each other (column 10, lines 46-57, column 11, lines 4-31 and column 12, lines 6-12);

D. if the compared result is that Y and X are equal, indicating the data that has not been falsified, and otherwise indicating that the data has been falsified (column 10, lines 46-57, column 11, lines 4-31 and column 12, lines 6-12).

18. Regarding claims 11 and 20, Thomlinson teaches using randomly changeable session key to encrypt the data during the data transmission (column 9, lines 66 and 67, column 10, lines 1-14 and 22-38).

19. Regarding claims 12 and 21, Thomlinson teaches that the step of using randomly changeable session key to encrypt data comprises the steps of:

A. at the beginning of the data transmission, transmission end transmitting a request of exchanging session key and introducing at least one random number (column 9, lines 66 and 67, column 10, lines 1-14 and 22-38);

B. after receiving the exchanging session key request, the semiconductor memory device randomly creating at least one random number, converting the received random number and the created random number by a key generating algorithm to produce a session key, and then returning the random number created by the semiconductor memory device to the transmission end (column 9, lines 66 and 67, column 10, lines 1-14 and 22-38);

C. after the transmission end receives the returned random number, converting the returned random number and the random number introduced by the transmission end itself with the key generating algorithm to produce the session key (column 9, lines 66 and 67, column 10, lines 1-14 and 22-38).

20. Regarding claim 13, Thomlinson teaches that the data to be protected include documents, passwords, cipher keys, account numbers, digital certificates, encrypting algorithm, self-defined algorithm, user information and user self-defined data (column 2, lines 28-44 and 60-67, column 3, lines 1-21, column 4, lines 45-67, column 5, lines 1-18, column 6, lines 10-39 and 47-53, column 7, lines 41-53 and 64-67, column 8, lines 1-29 and 41-57, column 9, lines l-6, 31-37 and 59-63 and column 10, lines 1-14 and 30-50, "the storage server stores the encrypted individual data item, the item authentication code, the encrypted item key, the encrypted item authentication key, the key authentication code, the encrypted master key, and the encrypted master authentication key, to be retrieved later when requested by an authorized application program").

21. Regarding claim 14, Thomlinson teaches wherein the semiconductor memory device comprises a controller module, and a universal interface module and a semiconductor storage medium module that electrically connected with the controller module, respectively, characterized in that the method comprises the steps of: dividing the semiconductor storage medium module into at least two logic memory spaces (column 4, lines 45-55, "system memory includes read only memory (ROM) 24 and random access memory (RAM) 25" and column 7, lines 25-32, "a dynamically linked library (DLL) that can be executed in the application programs' address spaces");

the controller module receiving input data from the universal interface (column 2, lines 16-23, column 3, lines 7-15, column 6, lines 10-35, "the protected storage system allows application programs to securely store data items that must be kept private and free from tampering", column 7, lines 15-21, "the protected storage system is implemented in a different address space than the calling application programs", column 9, lines 31-43 and column 11, lines 28-35).

22. Thomlinson significantly teaches the claimed invention, as cited above. However, Thomlinson does not substantially teach the claim language pertaining to the storing of an algorithm. Lys teaches said claim language, as cited below.

23. Regarding claim 14, Lys teaches a method for realizing algorithm storage by means of a semiconductor memory device, using at least one of the logic memory spaces for storing an algorithm the controller module executing a designated algorithm according to the input data, and transmitting a result of the execution via the universal interface (column 16, lines 6-16 and column 18, lines 36-49).

24. The motivation to combine would be provide a means "to select a program from memory, modify a program from memory, modify a program parameter from memory, select an external signal or provide other user interface solutions." (*Lys* – column 16, lines 13-16).

25. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Lys with the teachings of Thomlinson to provide a means to store the appropriate instructions to execute various functions.

26. Regarding claim 16, Thomlinson teaches that the algorithm is an algorithm *or* several algorithms (column 2, lines 28-44 and 60-67, column 3, lines 1-21, column 4, lines 45-67, column 5, lines 1-18, column 6, lines 10-39 and 47-53, column 7, lines 41-53, column 9, lines 31-37 and 59-63)

27. Regarding claim 17, Thomlinson teaches that the algorithm is an algorithm built in the semiconductor memory device *or* a self-defined algorithm *or* an encrypting algorithm (column 11, lines 11-24, "hard-coded into the various modules of the server and providers").

Conclusion

28. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

29. The following United States Patents are cited to further show the state of the art with respect to secure data protection, such as:

United States Patent No. 7,047,416 to Wheeler et al., which is cited to show an account-based digital signature (ABDS) system.

United States Patent No. 5,864,683 to Boebert et al., which is cited to show a system for providing secure internetwork by connecting type enforcing secure computers to external network for limiting access to data based on user and process access rights.

United States Patent No. 6,832,317 to Strongin et al., which is cited to show a personal computer security mechanism.

United States Patent No. 7,065,654 to Gulick et al., which is cited to show a secure execution box.

United States Patent No. 6,934,836 to Strand et al., which is cited to show a fluid separation conduit cartridge with encryption capability.

United States Patent No. 6,757,832 to Silverbrook et al., which is cited to show unauthorized modification of values in flash memory.

United States Patent No. 6,816,968 to Walmsley, which is cited to show a consumable authentication protocol and system.

United States Patent No. 6,721,891 to Borza, which is cited to show a method of distributing piracy protected computer software.

United States Patent No. 6,698,654 to Zuppicich which is cited to show a method of interfacing with data storage card.

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

31. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

32. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431